(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（A）**　(11)特許出願公開番号

特開平11－53668

(43)公開日　平成11年(1999)２月26日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０８Ｂ	25/04		Ｇ０８Ｂ	25/04	Ｋ
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ｂ
	17/30		Ｈ０４Ｍ	11/04	
Ｈ０４Ｌ	12/437		Ｇ０６Ｆ	15/40	３１０Ｆ
	12/02		Ｈ０４Ｌ	11/00	３３１

審査請求　未請求　請求項の数６　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願平9－206177

(22)出願日　平成９年(1997)７月31日

(71)出願人　000237156
株式会社エフ・エフ・シー
東京都日野市富士町１番地

(72)発明者　西田　廣治
東京都日野市富士町１番地　富士ファコム制御株式会社内

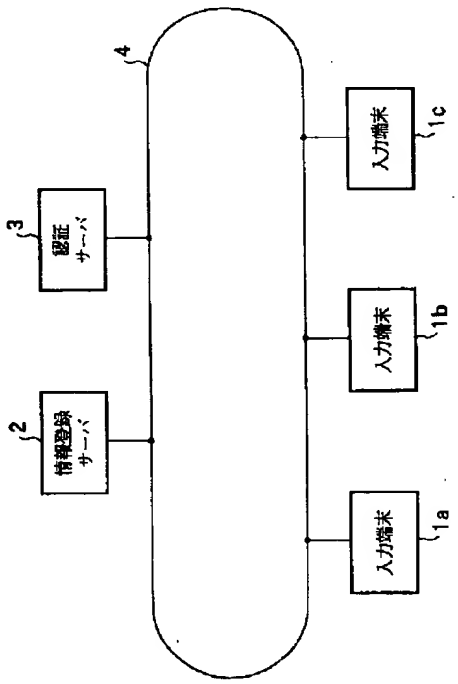
(74)代理人　弁理士　森　哲也　（外３名）

(54)【発明の名称】　災害時情報システム

(57)【要約】

【課題】　災害発生の際に、救助活動や復旧活動を適切かつ早急に行うために必要な個人情報を好適に提供することのできる災害時情報システムを提供する。

【解決手段】　個人に関する個人情報として、少なくとも医療に必要な身体情報および住所または居所に関する所在情報を入力して暗号化する入力端末と、入力端末で暗号化された個人情報を登録する個人情報登録装置と、を接続し、災害発生の際に、個人情報登録装置に登録されている個人情報を特定者に復号化して提供する。



1

【特許請求の範囲】

【請求項１】　個人に関する個人情報として、医療行為に必要な身体情報及び住所又は居所に関する所在情報を少なくとも入力して暗号化する入力端末と、前記入力端末で暗号化された前記個人情報を登録する個人情報登録装置と、を接続し、災害発生の際に、前記個人情報登録装置に登録されている前記個人情報を特定者に復号化して提供することを特徴とする災害時情報システム。

【請求項２】　個人に関する個人情報として、医療行為に必要な身体情報及び住所又は居所に関する所在情報を少なくとも入力するための入力端末と、前記入力端末で入力された前記個人情報を登録する個人情報登録装置と、をネットワークに接続し、

前記入力端末は、入力された前記個人情報を特定の暗号キーで暗号化する暗号化処理と、前記暗号化処理により暗号化された前記個人情報を前記個人情報登録装置に送信する送信処理と、を実行し、且つ、前記個人情報を利用する適格を有する特定者の要求に応じて前記個人情報登録装置から前記個人情報を取得する取得処理と、前記取得処理により取得された前記個人情報を前記特定の暗号キーに対応する特定の復号キーで復号化する復号化処理と、を実行し、

前記個人情報登録装置は、前記入力端末から送信された前記個人情報を登録する登録処理と、災害発生の際に前記入力端末からの要求に応じて前記登録処理により登録された前記個人情報を前記入力端末に提供する提供処理と、を実行することを特徴とする災害時情報システム。

【請求項３】　前記個人情報を送信しようとする先が前記個人情報登録装置であるか否かを認証するための第１の認証装置を前記ネットワークに接続し、

前記入力端末は、前記第１の認証装置を利用し、前記個人情報を送信しようとする先が前記個人情報登録装置であると認証したときに、前記送信処理を実行することを特徴とする請求項２記載の災害時情報システム。

【請求項４】　前記個人情報には、前記個人の安否に関する安否情報が含まれていることを特徴とする請求項１、２又は３記載の災害時情報システム。

【請求項５】　前記個人と特定の関係を有する関係者の公開鍵を登録した第２の認証装置を前記ネットワークに接続し、

前記入力端末は、前記取得処理を実行する際に、前記関係者から入力された前記公開鍵に対応する秘密鍵で暗号化した認証情報を前記個人情報登録装置に送信し、前記個人情報登録装置から前記個人情報を取得したときに、前記個人情報を前記秘密鍵で復号化し、

前記個人情報登録装置は、前記入力端末から前記認証情報が送信された場合に、前記第２の認証装置から前記関係者の前記公開鍵を取得し、取得した前記公開鍵で前記認証情報を復号化し、前記認証情報が正常に復号化されたときに、前記個人情報を前記公開鍵で暗号化して前記

2

入力端末に提供することを特徴とする請求項２、３又は４記載の災害時情報システム。

【請求項６】　前記関係者の金銭の額を管理する金額管理装置を前記ネットワークに接続し、

前記入力端末は、災害発生の際に、前記関係者の要求に応じて前記金額管理装置で管理されている前記関係者の金銭の額を義援金として提供することを特徴とする請求項５記載の災害時情報システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術の分野】本発明は、災害発生の際に、あらかじめ登録した個人情報を、その利用適格を有する特定者に提供する災害時情報システムに関する。

【０００２】

【従来の技術】従来、個人に関する情報として、病院のカルテに記載される医療情報や自己所有の金銭の額に関する金額情報、住所または居所の建物の間取り図や緊急連絡先などは、その多くが紙面や狭域内に設けられたデータベースなどに記録され、それぞれ独立に管理されていた。

【０００３】

【発明が解決しようとする課題】ところで、従来、災害発生の際には、これら個人情報を利用することにより、医療活動に従事する医師や救護活動に従事する救護員または消防要員などが適切に救助活動を行えたり、本人またはその家族等が早急に復旧活動を行えたりすることが望まれていた。

【０００４】しかしながら、病院のカルテに記載される医療情報や自己所有の金銭の額に関する金額情報などの個人情報は、病院内や銀行間でのみ利用が限定されたデータベースにより管理されており、しかも、個人情報を利用する権限を有する者でなければ、例え家族等であっても利用することができない場合があった。

【０００５】また、情報が統括して管理されていないため、医療活動に従事する医師や救護活動に従事する救急要員または消防要員、本人や家族等は、必要な情報ごとに、その情報があるところまで赴かなければ、これを得ることができなかった。

【０００６】そこで、本発明は、このような従来の問題を解決することを課題としており、災害発生の際に、救助活動や復旧活動を適切かつ早急に行うために必要な個人情報を好適に提供することのできる災害時情報システムを提供することを目的としている。

【０００７】

【課題を解決するための手段】上記目的を達成するために、本発明に係る請求項１記載の災害時情報システムは、個人に関する個人情報として、医療行為に必要な身体情報および住所または居所に関する所在情報を少なくとも入力して暗号化する入力端末と、前記入力端末で暗号化された前記個人情報を登録する個人情報登録装置

と、を接続し、災害発生の際に、前記個人情報登録装置に登録されている前記個人情報を特定者に復号化して提供する。

【０００８】このような構成であれば、災害が発生していない通常のときには、本人、家族等、医師、公営機関または建築業者などが入力端末を利用し、医療情報や所在情報などの個人情報を入力する。そうすると、入力端末では、入力された個人情報が暗号化されて個人情報登録装置に送信される。個人情報登録装置では、入力端末から送信された個人情報が登録される。

【０００９】一方、災害が発生したときには、個人情報を利用する適格を有する特定者が入力端末を利用し、個人情報の提供を要求する。そうすると、入力端末では、特定者からの要求に応じて、個人情報登録装置に対して個人情報の提供が要求される。個人情報登録装置では、個人情報の提供を要求している者が特定者であると確認されたときに、登録されている個人情報が入力端末に提供される。そして、このとき、提供される個人情報は、入力端末または個人情報登録装置で復号化されて特定者に提供される。

【００１０】なお、災害が発生していない通常のときに限らず、いかなるときであっても、個人情報を入力端末に入力して個人情報登録装置に登録するようにしてもよいし、災害が発生していない通常のときにのみ、個人情報を入力端末に入力して個人情報登録装置に登録するようにしてもよい。

【００１１】この請求項１記載の発明において、身体情報とは、医療行為に必要な情報であって、例えば、病院のカルテに記載される情報である。また、所在情報とは、住所または居所に関する情報であって、例えば、住所若しくは居所そのもの、住所若しくは居所に係る電話番号、住所若しくは居所に係る建物の間取り図、住所若しくは居所を含む周辺の地図、または緊急連絡先である。さらに、特定者とは、個人情報を利用する適格を有する者であって、例えば、本人若しくは家族等、または、災害発生の際に、医療活動に従事する医師、救護活動に従事する救護員、国若しくは救助活動を指揮する地方自治体の責任者である。

【００１２】また、本発明に係る請求項２記載の災害時情報システムは、個人に関する個人情報として、医療行為に必要な身体情報および住所または居所に関する所在情報を少なくとも入力するための入力端末と、前記入力端末で入力された前記個人情報を登録する個人情報登録装置と、をネットワークに接続し、前記入力端末は、入力された前記個人情報を特定の暗号キーで暗号化する暗号化処理と、前記暗号化処理により暗号化された前記個人情報を前記個人情報登録装置に送信する送信処理と、を実行し、かつ、前記個人情報を利用する適格を有する特定者の要求に応じて前記個人情報登録装置から前記個人情報を取得する取得処理と、前記取得処理により取得された前記個人情報を前記特定の暗号キーに対応する特定の復号キーで復号化する復号化処理と、を実行し、前記個人情報登録装置は、前記入力端末から送信された前記個人情報を登録する登録処理と、災害発生の際に前記入力端末からの要求に応じて前記登録処理により登録された前記個人情報を前記入力端末に提供する提供処理と、を実行する。

【００１３】このような構成であれば、災害が発生していない通常のときには、本人、家族等、医師、公営機関または建築業者などが入力端末を利用し、医療情報や所在情報などの個人情報を入力する。そうすると、入力端末では、暗号化処理により、入力された個人情報が特定の暗号キーで暗号化され、送信処理により、暗号化された個人情報が個人情報登録装置に送信される。個人情報登録装置では、登録処理により、入力端末から送信された個人情報が登録される。

【００１４】一方、災害が発生したときには、個人情報を利用する適格を有する特定者が入力端末を利用し、個人情報の提供を要求する。そうすると、入力端末では、特定者からの要求に応じて、取得処理により、個人情報登録装置に対して個人情報の提供が要求される。個人情報登録装置では、個人情報の提供を要求している者が特定者であると確認されたときに、提供処理により、登録されている個人情報が入力端末に提供される。そして、入力端末では、取得処理により、個人情報登録装置から個人情報が取得され、復号化処理により、取得された個人情報が特定の復号キーで復号化される。これにより、個人情報が特定者に提供される。

【００１５】この請求項２記載の発明において、暗号キーとは、データを暗号化しようとするアルゴリズムを決定するための動機付けとなるものである。また、暗号キーと対応する復号キーとは、暗号化されているデータを復号化しようとするアルゴリズムを決定するための動機付けとなるものであって、暗号キーとデータを正常に復元するために必要な所定の因果関係を有するものである。これらには、データを暗号化するとき、または、暗号化データを復号化するときに設定するパスワードや、パスワードを要しない暗号化または復号化アルゴリズムであれば、そのアルゴリズムそのものをも含むものである。

【００１６】したがって、この請求項２記載の発明において、復号化とは、暗号化データの暗号キーと上記所定の因果関係を有している復号キーに基づいて、暗号化データを元のデータに正常に復元することであって、その暗号キーと上記所定の因果関係を有していない復号キーに基づいて、元のデータ以外のものを生成することは含まないものである。

【００１７】さらに、本発明に係る請求項３記載の災害時情報システムは、請求項２記載の災害時情報システムにおいて、前記個人情報を送信しようとする先が前記個

人情報登録装置であるか否かを認証するための第１の認証装置を前記ネットワークに接続し、前記入力端末は、前記第１の認証装置を利用し、前記個人情報を送信しようとする先が前記個人情報登録装置であると認証したときに、前記送信処理を実行する。

【００１８】このような構成であれば、入力端末では、入力された個人情報が暗号化されると、第１の認証装置が利用され、個人情報を送信しようとする先が個人情報登録装置であるか否かが認証される。そして、送信しようとする先が個人情報登録装置であると認証されたときに、送信処理により、暗号化した個人情報が個人情報登録装置に送信される。

【００１９】この場合において、個人情報登録装置を認証するには、例えば、第１の認証装置にあらかじめ正当な個人情報登録装置であることを示すための公開鍵を登録しておき、個人情報登録装置が登録してある公開鍵に対応する秘密鍵で認証情報を暗号化して入力端末に送信する。入力端末では、個人情報登録装置から認証情報を受信したときに、第１の認証装置から登録してある個人情報登録装置の公開鍵を取得し、その公開鍵で送信された認証情報を復号化し、正常に復号化することができるか否かを判定するようにすればよい。

【００２０】個人に関する個人情報は、プライバシーに係わる情報であるため、厳重にその機密を保護しなければならない。入力端末と個人情報登録装置とが専用回線で接続されているような場合には特に問題はないが、インターネットなど複数のコンピュータが接続されているようなネットワークにこれらを接続するような場合には、入力端末が誤って異なるコンピュータに個人情報を送信してしまうおそれがある。そこで、上記のように、入力端末で、送信しようとする先が個人情報登録装置であるか否かを認証してから個人情報を送信するようにすれば、個人情報が漏洩する可能性を低減することができる。

【００２１】さらに、本発明に係る請求項４記載の災害時情報システムは、請求項１、２または３記載の災害時情報システムにおいて、前記個人情報には、前記個人の安否に関する安否情報が含まれている。

【００２２】さらに、本発明に係る請求項５記載の災害時情報システムは、請求項２、３または４記載の災害時情報システムにおいて、前記個人と特定の関係を有する関係者の公開鍵を登録した第２の認証装置を前記ネットワークに接続し、前記入力端末は、前記取得処理を実行する際に、前記関係者から入力された前記公開鍵に対応する秘密鍵で暗号化した認証情報を前記個人情報登録装置に送信し、前記個人情報登録装置から前記個人情報を取得したときに、前記個人情報を前記秘密鍵で復号化し、前記個人情報登録装置は、前記入力端末から前記認証情報が送信された場合に、前記第２の認証装置から前記関係者の前記公開鍵を取得し、取得した前記公開鍵で前記認証情報を復号化し、前記認証情報が正常に復号化されたときに、前記個人情報を前記公開鍵で暗号化して前記入力端末に提供する。

【００２３】このような構成であれば、個人と特定の関係を有する家族等の関係者が個人情報を取得しようとするには、関係者が入力端末を利用し、個人情報の提供を要求する。そうすると、入力端末では、関係者から入力された秘密鍵で認証情報が暗号化され、暗号化された認証情報が個人情報登録装置に送信される。個人情報登録装置では、個人情報の提供を要求した者の公開鍵が第２の認証装置から取得され、送信された認証情報が取得された公開鍵で復号化される。このとき、認証情報が正常に復号化されると、個人情報の提供を要求した者が個人情報を利用する適格を有する関係者であるものと判定され、該当する個人情報が公開鍵で暗号化され、入力端末に提供される。入力端末では、認証情報を暗号化したときと同一の秘密鍵で提供された個人情報が復号化される。これにより、個人情報が関係者に提供される。

【００２４】さらに、本発明に係る請求項６記載の災害時情報システムは、請求項５記載の災害時情報システムにおいて、前記関係者の金銭の額を管理する金額管理装置を前記ネットワークに接続し、前記入力端末は、災害発生の際に、前記関係者の要求に応じて前記金額管理装置で管理されている前記関係者の金銭の額を義援金として提供する。

【００２５】このような構成であれば、災害が発生したときに、関係者が被災地に義援金を提供しようとするには、関係者が入力端末を利用し、義援金を提供することを要求する。そうすると、入力端末では、関係者からの要求に応じて、金額管理装置に対して義援金の支払いが要求される。金額管理装置では、義援金の支払いが要求されると、支払いを要求した関係者が所有する金銭の額が義援金として提供される。

【００２６】従来、義援金を提供しようとする者は、銀行や郵便局などを利用して義援金を被災地に提供していた。しかし、銀行や郵便局などに赴くために労力を要したり、またそこでの手続きが必要であったりすることなどが義援金を提供しようとする者を億劫にさせてしまい、積極的な義援活動が行われているとは言いがたかった。そこで、このように入力端末を利用することにより、簡単に義援金を提供できるようにすれば、多大な義援金の提供が期待され、支援活動が有効に行われることが期待される。

【００２７】この請求項５記載の発明において、金額管理装置で管理される金銭の額とは、例えば、銀行の口座等で管理されるキャッシュ情報やクレジット情報である。

【００２８】

【発明の実施の形態】以下、本発明の第１の実施の形態を図面を参照しながら説明する。図１は、本発明に係る

災害時情報システムによる第１の実施の形態を示すブロック図である。

【００２９】この第１の実施の形態は、本発明に係る災害時情報システムを、図１に示すように、各地に設置された入力端末と、情報登録サーバと、認証サーバと、をネットワークに接続し、各入力端末で個人に関する個人情報を入力するとともに、災害発生の際に、登録されている個人情報を利用するのに適用したものである。

【００３０】図中、個人情報を入力し且つ災害発生の際に個人情報を利用するための入力端末１ａ～１ｃと、入力端末１ａ～１ｃで入力された個人情報を登録し且つ災害発生の際に登録した個人情報を入力端末１ａ～１ｃに提供する情報登録サーバ２と、入力端末１ａ～１ｃおよび情報登録サーバ２間で送受信されるデータを認証するための認証サーバ３とは、データを伝送するためのデータ伝送路４で相互に接続されている。

【００３１】入力端末１ａ～１ｃ、情報登録サーバ２および認証サーバ３は、図２に示すように、同一機能を有して構成されており、演算およびシステム全体を制御する演算処理装置５と、データの読み出しおよび書き込みが可能な主記憶装置６および補助記憶装置７と、外部からのデータ入力が可能なヒューマンインターフェースとしてのキーボード８と、キーボード８および外部とのデータの入出力を行うインターフェース部９と、主記憶装置６の特定領域に格納されているデータを画像信号に変換して出力するＣＲＴ制御装置１０と、ＣＲＴ制御装置１０から出力された画像信号を画面に表示するＣＲＴ１１と、で構成されており、演算処理装置５、主記憶装置６、補助記憶装置７およびインターフェース部９は、データを伝送するための信号線であるバスで相互に接続されている。

【００３２】主記憶装置６は、あらかじめ演算処理装置５の制御プログラム等が格納されているＲＯＭと、補助記憶装置７から読み込んだデータおよび演算処理装置５の演算過程で必要な演算結果を格納するＲＡＭと、ＣＲＴ１１に表示するための表示データを蓄積するＶＲＡＭと、で構成されている。なお、ＶＲＡＭは、演算処理装置５とＣＲＴ制御装置１０とで独立に、かつ、相互にアクセスが可能となっている。

【００３３】補助記憶装置７は、ＦＤＤまたはＨＤＤ等の不揮発性記憶媒体からなっている。そして、情報登録サーバ２の補助記憶装置７には、図３に示すように、入力端末１ａ～１ｃから送信される個人情報が格納されるようになっている。この場合に、個人情報は、個人情報に係る者の名前と、医療に必要な身体情報と、住所および居所やその電話番号などの連絡先情報と、住所および居所に係る建物の間取り図などの建物構造情報と、からなっている。また、認証サーバ３の補助記憶装置７には、図４に示すように、情報登録サーバ２に登録されている個人情報に係る者の名前と、その公開鍵と、が格納されるようになっている。

【００３４】ＣＲＴ制御装置１０は、主記憶装置６のＶＲＡＭに格納されているデータを先頭アドレスから所定周期で順次読み出し、読み出したデータを画像信号に変換してＣＲＴ１１に出力するように構成されている。

【００３５】入力端末１ａ～１ｃの演算処理装置５は、マイクロプロセッシングユニットＭＰＵ等からなり、個人情報を入力しようとするときには、主記憶装置６のＲＯＭの所定領域に格納されている所定のプログラムを起動させ、図５（ａ）のフローチャートに示す処理を実行し、災害発生の際に、情報登録サーバ２に登録されている個人情報を利用しようとするときには、図５（ｂ）のフローチャートに示す処理を実行するようになっている。

【００３６】つまり、入力端末１ａ～１ｃの演算処理装置５で、個人情報を入力しようとするときに実行される処理は、次のように構成されている。まず、図５（ａ）に示すように、ステップＳ１に移行して、個人情報をキーボード８より入力し、ステップＳ２に移行して、入力した個人情報に係る者の公開鍵をキーボード８より入力し、ステップＳ３に移行して、入力した個人情報に係る者の公開鍵で個人情報を暗号化し、ステップＳ４に移行するようになっている。

【００３７】ステップＳ４では、情報登録サーバ２より認証情報を取得し、ステップＳ５に移行して、認証サーバ３より情報登録サーバ２の公開鍵を取得し、ステップＳ６に移行して、取得した情報登録サーバ２の公開鍵で認証情報を復号化し、ステップＳ７に移行するようになっている。なお、ステップＳ４で、情報登録サーバ２より取得する認証情報は、情報登録サーバ２の秘密鍵で暗号化されている。

【００３８】ステップＳ７では、認証情報が正常に復号化されたか否かを判定し、正常に復号化されたと判定されたときには、ステップＳ８に移行して、そうでないと判定されたときには、ステップＳ４に移行するようになっている。ここで、取得される認証情報は、あらかじめ設定した所定の書式に基づいて作成されたものであり、正常に復号化されたか否かを判定するには、復号化した結果、所定の書式が検出されるか否かによって行うようになっている。

【００３９】ステップＳ８では、暗号化した個人情報を情報登録サーバ２に送信し、一連の処理を終了するようになっている。また、入力端末１ａ～１ｃの演算処理装置５で、災害発生の際に、情報登録サーバ２に登録されている個人情報を利用しようとするときに実行される処理は、次のように構成されている。まず、図５（ｂ）に示すように、ステップＳ１１に移行して、要求する個人情報に係る者の名前をキーボード８より入力し、ステップＳ１２に移行して、要求する個人情報に係る者の秘密鍵をキーボード８より入力し、ステップＳ１３に移行し

て、要求する個人情報に係る者の秘密鍵で認証情報を暗号化し、ステップＳ１４に移行するようになっている。

【００４０】ステップＳ１４では、暗号化した認証情報を情報登録サーバ２に送信し、ステップＳ１５に移行して、情報登録サーバ２より個人情報を受信したか否かを判定し、受信したと判定されたときには、ステップＳ１６に移行して、要求する個人情報に係る者の秘密鍵で受信した個人情報を復号化し、ステップＳ１７に移行して、復号化した個人情報をＣＲＴ１１に表示し、一連の処理を終了するようになっている。

【００４１】一方、ステップＳ１５で、情報登録サーバ２より個人情報を受信しないと判定されたときには、ステップＳ１８に移行して、所定のエラー処理を実行し、一連の処理を終了するようになっている。

【００４２】また一方、情報登録サーバ２の演算処理装置５は、マイクロプロセッシングユニットＭＰＵ等からなり、入力端末１ａ～１ｃより個人情報の登録が要求されたときには、主記憶装置６のＲＯＭの所定領域に格納されている所定のプログラムを起動させ、図６（ａ）のフローチャートに示す処理を実行し、災害発生の際に、入力端末１ａ～１ｃより個人情報の提供が要求されたときには、図６（ｂ）のフローチャートに示す処理を実行するようになっている。

【００４３】つまり、情報登録サーバ２の演算処理装置５で、入力端末１ａ～１ｃより個人情報の登録が要求されたときに実行される処理は、次のように構成されている。まず、図６（ａ）に示すように、ステップＳ２１に移行して、情報登録サーバ２の秘密鍵で認証情報を暗号化し、ステップＳ２２に移行して、暗号化した認証情報を登録要求のあった入力端末１ａ～１ｃに送信し、ステップＳ２３に移行するようになっている。

【００４４】ステップＳ２３では、登録要求のあった入力端末１ａ～１ｃより個人情報を受信したか否かを判定し、受信したと判定されたときには、ステップＳ２４に移行して、受信した個人情報を補助記憶装置７の所定領域に登録し、一連の処理を終了するようになっている。

【００４５】一方、ステップＳ２３で、登録要求のあった入力端末１ａ～１ｃより個人情報を受信しないと判定されたときには、ステップＳ２５に移行して、所定のエラー処理を実行し、一連の処理を終了するようになっている。

【００４６】また、情報登録サーバ２の演算処理装置５で、災害発生の際に、入力端末１ａ～１ｃより個人情報の提供が要求されたときに実行される処理は、次のように構成されている。まず、図６（ｂ）に示すように、ステップＳ３１に移行して、入力端末１ａ～１ｃより送信される認証情報を受信し、ステップＳ３２に移行して、要求のあった個人情報に係る者の公開鍵を認証サーバ３より取得し、ステップＳ３３に移行するようになっている。

【００４７】ステップＳ３３では、要求のあった個人情報に係る者の公開鍵で認証情報を復号化し、ステップＳ３４に移行して、認証情報が正常に復号化されたか否かを判定し、正常に復号化されたと判定されたときには、ステップＳ３５に移行して、該当する個人情報を要求のあった入力端末１ａ～１ｃに送信し、一連の処理を終了するようになっている。

【００４８】一方、ステップＳ３４で、認証情報が正常に復号化されないと判定されたときには、ステップＳ３６に移行して、所定のエラー処理を実行し、一連の処理を終了するようになっている。

【００４９】また一方、認証サーバ３の演算処理装置５は、マイクロプロセッシングユニットＭＰＵ等からなり、入力端末１ａ～１ｃおよび情報登録サーバ２より公開鍵の提供要求がされたときには、主記憶装置６のＲＯＭの所定領域に格納されている所定のプログラムを起動させ、要求のあった個人情報に係る者の名前に該当する公開鍵を補助記憶装置７から読み込み、要求のあった入力端末１ａ～１ｃまたは情報登録サーバ２に送信するようになっている。

【００５０】次に、上記第１の実施の形態の動作を図面を参照しながら説明する。始めに、災害が発生していない通常のときに、本人、家族等、医師、公営機関または建築業者などがいずれかの入力端末１ａ～１ｃを利用し、個人情報を情報登録サーバ２に登録する場合について説明する。

【００５１】まず、本人、家族等、医師、公営機関または建築業者などが個人情報を情報登録サーバ２に登録しようとするには、各地に設置されているいずれかの入力端末１ａ～１ｃ、例えば入力端末１ａを利用し、個人情報に係る者の名前、身体情報、連絡先情報または建物構造情報などの個人情報を入力するとともに、個人情報に係る者の公開鍵を入力する。

【００５２】そうすると、入力端末１ａでは、入力された個人情報が暗号化され、ステップＳ４からＳ７までを経て、個人情報を送信しようとする先が情報登録サーバ２であるか否かが認証され、送信しようとする先が情報登録サーバ２であると認証されたときに、暗号化された個人情報が情報登録サーバ２に送信される。

【００５３】情報登録サーバ２では、入力端末１ａより個人情報が送信されると、補助記憶装置７にその個人情報が登録される。このとき、暗号化された個人情報は、図３に示すように、名前、身体情報、連絡先情報および建物構造情報のフィールドに区分され、個人情報ごとに１レコードとして登録される。

【００５４】なお、入力端末１ａでは、個人情報を送信しようとする先が情報登録サーバ２でないと認証されたときには、情報登録サーバ２であると認証されるまで、ネットワークに接続されたコンピュータに対して認証を実行し続ける。また、情報登録サーバ２では、入力端末

１ａより個人情報の登録要求があったにもかかわらず、入力端末１ａより個人情報が送信されないときには、エラー処理が実行される。

【００５５】その次に、災害が発生した際に、本人若しくは家族等、または、医療活動に従事する医師、救護活動に従事する救護員、国若しくは救助活動を指揮する地方自治体の責任者などの個人情報を利用する適格を有する者（以下、特定者と称する）が、情報登録サーバ２に登録されている個人情報を救助活動等のために利用しようとする場合について説明する。

【００５６】まず、特定者が情報登録サーバ２に登録されている個人情報を利用するには、各地に設置されているいずれかの入力端末１ａ～１ｃ、例えば入力端末１ｂを利用し、利用しようとする個人情報に係る者の名前を入力するとともに、利用しようとする個人情報に係る者の秘密鍵を入力する。

【００５７】そうすると、入力端末１ｂでは、情報登録サーバ２に個人情報の提供が要求されるとともに、ステップＳ１３，Ｓ１４を経て、入力された秘密鍵に基づいて、情報登録サーバ２に対して個人情報を利用しようとする者が特定者であることが証明される。

【００５８】情報登録サーバ２では、ステップＳ３１からＳ３４までを経て、個人情報を利用しようとする者が特定者であると認証されると、該当する個人情報が入力端末１ｂに送信される。

【００５９】入力端末１ｂでは、情報登録サーバ２より個人情報が送信されると、個人情報に係る者の秘密鍵でその個人情報が復号化され、ＣＲＴ制御装置１０によりＣＲＴ１１に表示される。

【００６０】なお、情報登録サーバ２では、個人情報を利用しようとする者が特定者でないと認証されたときには、その旨が入力端末１ｂに送信される。入力端末１ｂでは、これを受信すると、エラー処理が実行される。

【００６１】このようにして、個人情報を入力して暗号化する入力端末１ａ～１ｃと、入力端末１ａ～１ｃで暗号化された個人情報を登録する情報登録サーバ２と、を接続し、災害発生の際に、情報登録サーバ２に登録されている個人情報を特定者に復号化して提供するようにしたから、救助活動や復旧活動を適切かつ早急に行うために必要な個人情報を好適に提供することができ、しかも、個人情報が漏洩する可能性を低減することができる。

【００６２】特に、入力端末１ａ～１ｃでは、入力された個人情報をその個人情報に係る者の公開鍵で暗号化し、暗号化した個人情報を情報登録サーバ２に送信するようにし、かつ、特定者の要求に応じて情報登録サーバ２から個人情報を取得し、取得した個人情報をその個人情報に係る者の秘密鍵で復号化するようにし、情報登録サーバ２では、入力端末１ａ～１ｃから送信された個人情報を登録し、災害発生の際に、入力端末１ａ～１ｃからの要求に応じて登録されている個人情報を入力端末１ａ～１ｃに提供するようにしたから、救助活動や復旧活動を適切かつ早急に行うために必要な個人情報をより好適に提供することができ、しかも、個人情報が漏洩する可能性をより低減することができる。

【００６３】また、個人情報を送信しようとする先が情報登録サーバ２であるか否かを認証するための認証サーバ３を前記ネットワークに接続し、入力端末１ａ～１ｃでは、認証サーバ３を利用し、個人情報を送信しようとする先が情報登録サーバ２であると認証したときに、個人情報を送信するようにしたから、入力端末１ａ～１ｃから情報登録サーバ２に個人情報を確実に送信することができ、個人情報が漏洩する可能性をさらに低減することができる。

【００６４】さらに、災害発生の際に、情報登録サーバ２に登録されている個人情報を利用しようとするときに、入力端末１ａ～１ｃと情報登録サーバ２とで、個人情報を利用しようとする者が特定者であるか否かを認証するようにしたら、特定者以外の者に個人情報が誤って提供される可能性を低減することができ、個人情報が漏洩する可能性をさらに低減することができる。

【００６５】次に、本発明の第２の実施の形態を説明する。この第２の実施の形態は、本発明に係る災害時情報システムを、図１に示すように、各地に設置された入力端末と、情報登録サーバと、認証サーバと、をネットワークに接続し、災害発生の際に、各入力端末で個人情報として個人の安否に関する安否情報を入力する一方で、登録されている安否情報を家族等が利用するのに適用したものであって、上記第１の実施の形態と同一に構成されている。

【００６６】認証サーバ３は、情報登録サーバ２に登録されている個人情報に係る者と特定の関係を有する家族等の関係者の公開鍵を登録するようになっている。入力端末１ａ～１ｃの演算処理装置５は、安否情報を入力しようとするときには、図７（ａ）のフローチャートに示す処理を実行し、災害発生の際に、情報登録サーバ２に登録されている安否情報を利用しようとするときには、図７（ｂ）のフローチャートに示す処理を実行するようになっている。

【００６７】つまり、入力端末１ａ～１ｃの演算処理装置５で、安否情報を入力しようとするときに実行される処理は、次のように構成されている。まず、図７（ａ）に示すように、ステップＳ４１に移行して、安否情報をキーボード８より入力し、ステップＳ４２に移行して、情報登録サーバ２より認証情報を取得し、ステップＳ４３に移行するようになっている。

【００６８】ステップＳ４３では、認証サーバ３より情報登録サーバ２の公開鍵を取得し、ステップＳ４４に移行して、取得した情報登録サーバ２の公開鍵で認証情報を復号化し、ステップＳ４５に移行して、認証情報が正

常に復号化されたか否かを判定し、正常に復号化されたと判定されたときには、ステップＳ４６に移行して、そうでないと判定されたときには、ステップＳ４２に移行するようになっている。

【００６９】ステップＳ４６では、安否情報を情報登録サーバ２に送信し、一連の処理を終了するようになっている。また、入力端末１ａ～１ｃの演算処理装置５で、災害発生の際に、情報登録サーバ２に登録されている安否情報を利用しようとするときに実行される処理は、次のように構成されている。まず、図７（ｂ）に示すように、ステップＳ５１に移行して、要求する安否情報に係る者の名前をキーボード８より入力し、ステップＳ５２に移行して、安否情報を要求する者の秘密鍵をキーボード８より入力し、ステップＳ５３に移行して、安否情報を要求する者の秘密鍵で認証情報を暗号化し、ステップＳ５４に移行するようになっている。

【００７０】ステップＳ５４では、暗号化した認証情報を情報登録サーバ２に送信し、ステップＳ５５に移行して、情報登録サーバ２より安否情報を受信したか否かを判定し、受信したと判定されたときには、ステップＳ５６に移行して、安否情報を要求する者の秘密鍵で受信した安否情報を復号化し、ステップＳ５７に移行して、復号化した安否情報をＣＲＴ１１に表示し、一連の処理を終了するようになっている。

【００７１】一方、ステップＳ５５で、情報登録サーバ２より安否情報を受信しないと判定されたときには、ステップＳ５８に移行して、所定のエラー処理を実行し、一連の処理を終了するようになっている。

【００７２】また一方、情報登録サーバ２の演算処理装置５は、入力端末１ａ～１ｃより安否情報の登録が要求されたときには、図８（ａ）のフローチャートに示す処理を実行し、災害発生の際に、入力端末１ａ～１ｃより安否情報の提供が要求されたときには、図８（ｂ）のフローチャートに示す処理を実行するようになっている。

【００７３】つまり、情報登録サーバ２の演算処理装置５で、入力端末１ａ～１ｃより安否情報の登録が要求されたときに実行される処理は、次のように構成されている。まず、図８（ａ）に示すように、ステップＳ６１に移行して、情報登録サーバ２の秘密鍵で認証情報を暗号化し、ステップＳ６２に移行して、暗号化した認証情報を登録要求のあった入力端末１ａ～１ｃに送信し、ステップＳ６３に移行するようになっている。

【００７４】ステップＳ６３では、登録要求のあった入力端末１ａ～１ｃより安否情報を受信したか否かを判定し、受信したと判定されたときには、ステップＳ６４に移行して、受信した安否情報を補助記憶装置７の所定領域に登録し、一連の処理を終了するようになっている。

【００７５】一方、ステップＳ６３で、登録要求のあった入力端末１ａ～１ｃより安否情報を受信しないと判定されたときには、ステップＳ６５に移行して、所定のエラー処理を実行し、一連の処理を終了するようになっている。

【００７６】また、情報登録サーバ２の演算処理装置５で、災害発生の際に、入力端末１ａ～１ｃより安否情報の提供が要求されたときに実行される処理は、次のように構成されている。まず、図８（ｂ）に示すように、ステップＳ７１に移行して、入力端末１ａ～１ｃより送信される認証情報を受信し、ステップＳ７２に移行して、要求のあった者の公開鍵を認証サーバ３より取得し、ステップＳ７３に移行するようになっている。

【００７７】ステップＳ７３では、要求のあった者の公開鍵で認証情報を復号化し、ステップＳ７４に移行して、認証情報が正常に復号化されたか否かを判定し、正常に復号化されたと判定されたときには、ステップＳ７５に移行して、該当する安否情報を要求のあった者の公開鍵で暗号化し、ステップＳ７６に移行して、暗号化した安否情報を要求のあった入力端末１ａ～１ｃに送信し、一連の処理を終了するようになっている。

【００７８】一方、ステップＳ７４で、認証情報が正常に復号化されないと判定されたときには、ステップＳ７７に移行して、所定のエラー処理を実行し、一連の処理を終了するようになっている。

【００７９】次に、上記第２の実施の形態の動作を図面を参照しながら説明する。始めに、災害が発生した際に、本人、医師または公営機関などがいずれかの入力端末１ａ～１ｃを利用し、安否情報を情報登録サーバ２に登録する場合について説明する。

【００８０】まず、本人、医師または公営機関などが安否情報を情報登録サーバ２に登録しようとするには、各地に設置されているいずれかの入力端末１ａ～１ｃ、例えば入力端末１ａを利用し、安否情報を入力する。

【００８１】そうすると、入力端末１ａでは、安否情報を送信しようとする先が情報登録サーバ２であるか否かが認証され、送信しようとする先が情報登録サーバ２であると認証されたときに、入力された安否情報が情報登録サーバ２に送信される。

【００８２】情報登録サーバ２では、入力端末１ａより安否情報が送信されると、補助記憶装置７にその安否情報が登録される。なお、入力端末１ａでは、安否情報を送信しようとする先が情報登録サーバ２でないと認証されたときには、情報登録サーバ２であると認証されるまで、ネットワークに接続されたコンピュータに対して認証を実行し続ける。また、情報登録サーバ２では、入力端末１ａより安否情報の登録要求があったにもかかわらず、入力端末１ａより個人情報が送信されないときには、エラー処理が実行される。

【００８３】その次に、災害が発生した際に、個人情報に係る者と特定の関係を有する家族等の関係者が情報登録サーバ２に登録されている安否情報を利用しようとする場合について説明する。

【００８４】まず、家族等が情報登録サーバ２に登録されている安否情報を利用するには、各地に設置されているいずれかの入力端末１ａ～１ｃ、例えば入力端末１ｃを利用し、利用しようとする安否情報に係る者の名前を入力するとともに、安否情報を利用しようとする家族等の秘密鍵を入力する。

【００８５】そうすると、入力端末１ｃでは、情報登録サーバ２に安否情報の提供が要求されるとともに、入力された秘密鍵に基づいて、情報登録サーバ２に対して安否情報を利用しようとする者が利用適格を有する者（認証サーバ３に公開鍵を登録した家族等）であることが証明される。

【００８６】情報登録サーバ２では、安否情報を利用しようとする者が利用適格を有する者であると認証されると、該当する個人情報がその利用適格を有する者の公開鍵で暗号化され入力端末１ｃに送信される。

【００８７】入力端末１ｃでは、情報登録サーバ２より安否情報が送信されると、安否情報を利用しようとする家族等の秘密鍵でその安否情報が復号化され、ＣＲＴ制御装置１０によりＣＲＴ１１に表示される。

【００８８】なお、情報登録サーバ２では、安否情報を利用しようとする者が利用適格を有しない者であると認証されたときには、その旨が入力端末１ｃに送信される。入力端末１ｃでは、これを受信すると、エラー処理が実行される。

【００８９】このようにして、情報登録サーバ２に登録する個人情報には、個人の安否に関する安否情報を含ませるようにしたから、災害発生の際に、安否情報をその家族等に好適に提供することができる。

【００９０】また、入力端末１ａ～１ｃは、情報登録サーバ２から安否情報を取得する際に、家族等の秘密鍵で暗号化した認証情報を情報登録サーバ２に送信し、情報登録サーバ２から安否情報を取得したときに、安否情報を家族等の秘密鍵で復号化し、情報登録サーバ２は、入力端末１ａ～１ｃから認証情報が送信された場合に、認証サーバ３から家族等の公開鍵を取得し、取得した公開鍵で認証情報を復号化し、正常に復号化されたときに、安否情報を家族等の公開鍵で暗号化して入力端末１ａ～１ｃに提供するようにしたから、個人情報が漏洩する可能性を低減することができる。

【００９１】なお、上記第１および第２の実施の形態においては、個人情報および安否情報を送信しようとする先が情報登録サーバ２であることを認証してから、個人情報および安否情報を送信するように構成したが、これに限らず、情報登録サーバ２の認証を行わずに、個人情報および安否情報を送信するように構成してもよい。

【００９２】また、上記第２の実施の形態においては、安否情報を関係者の公開鍵で暗号化して入力端末１ａ～１ｃに提供するように構成したが、これに限らず、安否情報を特に暗号化しないで入力端末１ａ～１ｃに提供するように構成してもよい。

【００９３】さらに、上記第１および第２の実施の形態においては、個人情報を登録しおよび利用する構成と、安否情報を登録しおよび利用する構成とを別に構成したが、これに限らず、個人情報および安否情報をともに登録しおよび利用するように構成にしてもよい。

【００９４】さらに、上記第１および第２の実施の形態においては、入力端末１ａ～１ｃ、情報登録サーバ２および認証サーバ３のみをネットワークに接続するように構成したが、これに限らず、例えば、家族等の金銭の額を管理する請求項６記載の金額管理装置としての金額管理装置をネットワークに接続し、入力端末１ａ～１ｃは、災害発生の際に、特定者の要求に応じて金額管理装置で管理されている特定者の金銭の額を義援金として提供するように構成してもよい。このような構成であれば、簡単な手続きで義援金を提供することができる。

【００９５】さらに、上記第１および第２の実施の形態において、入力端末１ａ～１ｃおよび情報登録サーバ２の演算処理装置５で図５～図８のフローチャートに示す処理を実行するにあたってはいずれも、主記憶装置６のＲＯＭにあらかじめ格納されているプログラムを実行する場合について説明したが、これに限らず、これらの手順を示したプログラムが記憶された記憶媒体から、そのプログラムを主記憶装置６のＲＡＭに読み込んで実行するようにしてもよい。

【００９６】ここで、記憶媒体とは、ＲＡＭ、ＲＯＭ、ＦＤ、コンパクトディスク、ハードディスク、光磁気ディスクまたは紙等の記憶媒体であって、電子的、磁気的、光学的等の読み取り方法のいかんにかかわらず、コンピュータで読み取り可能な記憶媒体であれば、あらゆる記憶媒体を含むものである。

【００９７】さらに、上記第１および第２の実施の形態において、入力端末１ａ～１ｃおよび情報登録サーバ２の演算処理装置５で図５～図８のフローチャートに示す処理はいずれも、ソフトウェアで構成した場合について説明したが、これに代えて、比較回路、演算回路、論理回路等の電子回路を組み合わせるように構成してもよい。

【００９８】上記実施の形態において、情報登録サーバ２は、請求項１、２または５記載の個人情報登録装置に対応し、認証サーバ３は、請求項３記載の第１の認証装置または請求項４記載の第２の認証装置に対応している。

【００９９】また、ステップＳ２およびＳ３は、請求項２記載の暗号化処理に対応し、ステップＳ８は、請求項２記載の送信処理に対応し、ステップＳ１１からＳ１５までは、請求項２記載の取得処理に対応し、ステップＳ１６は、請求項２記載の復号化処理に対応し、ステップＳ２４は、請求項２記載の登録処理に対応し、ステップＳ３１からＳ３５までは、請求項２記載の提供処理に対

応している。

【０１００】

【発明の効果】以上説明したように、本発明に係る災害時情報システムによれば、救助活動や復旧活動を適切かつ早急に行うために必要な個人情報を好適に提供することができ、しかも、個人情報が漏洩する可能性を低減することができるという効果が得られる。

【０１０１】また、本発明に係る請求項２記載の災害時情報システムによれば、個人情報が漏洩する可能性をより低減することができるという効果も得られる。さらに、本発明に係る請求項３記載の災害時情報システムによれば、入力端末から個人情報登録装置に個人情報を確実に送信することができるから、個人情報が漏洩する可能性をさらに低減することができるという効果も得られる。

【０１０２】さらに、本発明に係る請求項４記載の災害時情報システムによれば、災害発生の際に、個人の安否に関する情報をその家族等に好適に提供することができるという効果も得られる。

【０１０３】さらに、本発明に係る請求項５記載の災害時情報システムによれば、個人情報が漏洩する可能性をさらに低減することができるという効果も得られる。さらに、本発明に係る請求項６記載の災害時情報システムによれば、簡単な手続きで義援金を提供することができるという効果も得られる。

【図面の簡単な説明】

【図１】第１の実施の形態の構成を示すブロック図である。

【図２】入力端末１ａ～１ｃ、情報登録サーバ２および認証サーバ３の構成を示すブロック図である。

【図３】認証サーバ３における特定者の公開鍵の登録方式を示す図である。

【図４】情報登録サーバ２における個人情報の登録方式を示す図である。

【図５】入力端末１ａ～１ｃの演算処理装置５で実行される処理を示すフローチャートである。

【図６】情報登録サーバ２の演算処理装置５で実行される処理を示すフローチャートである。

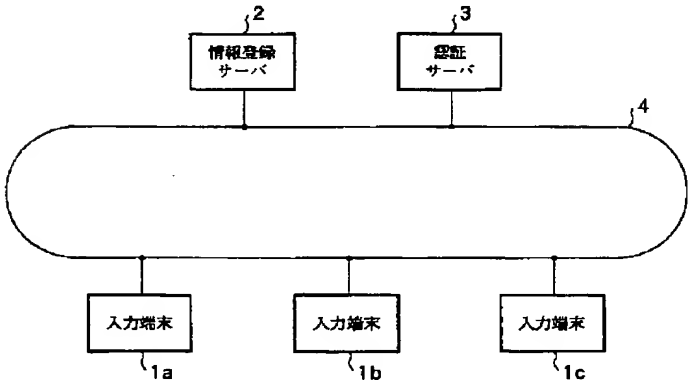
【図７】入力端末１ａ～１ｃの演算処理装置５で実行される処理を示すフローチャートである。

【図８】情報登録サーバ２の演算処理装置５で実行される処理を示すフローチャートである。

【符号の説明】

１ａ～１ｃ	入力端末
２	情報登録サーバ
３	認証サーバ
４	データ伝送路
５	演算処理装置
６	主記憶装置
７	補助記憶装置
８	キーボード
９	インターフェース部
１０	ＣＲＴ制御装置
１１	ＣＲＴ

【図１】



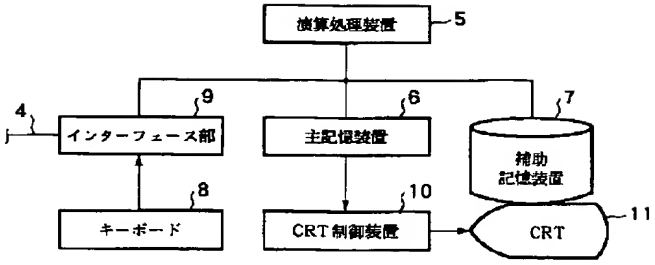
【図３】

名前	身体情報	連絡先情報	建物構造情報
A	M_1	A_1	S_1
B	M_2	A_2	S_2
C	M_3	A_3	S_3
≈	≈	≈	≈
Z	M_n	A_n	S_n

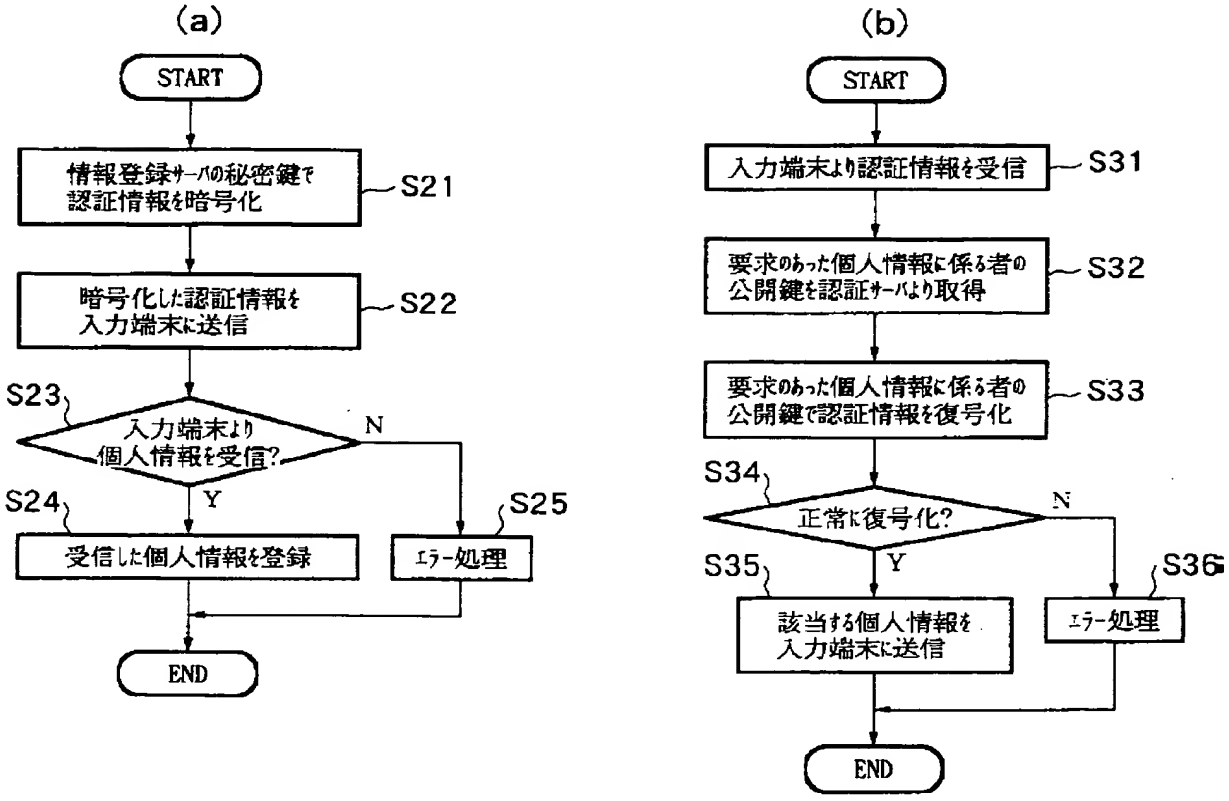
【図４】

名前	公開鍵
A	KO_1
B	KO_2
C	KO_3
≈	≈
Z	KO_n

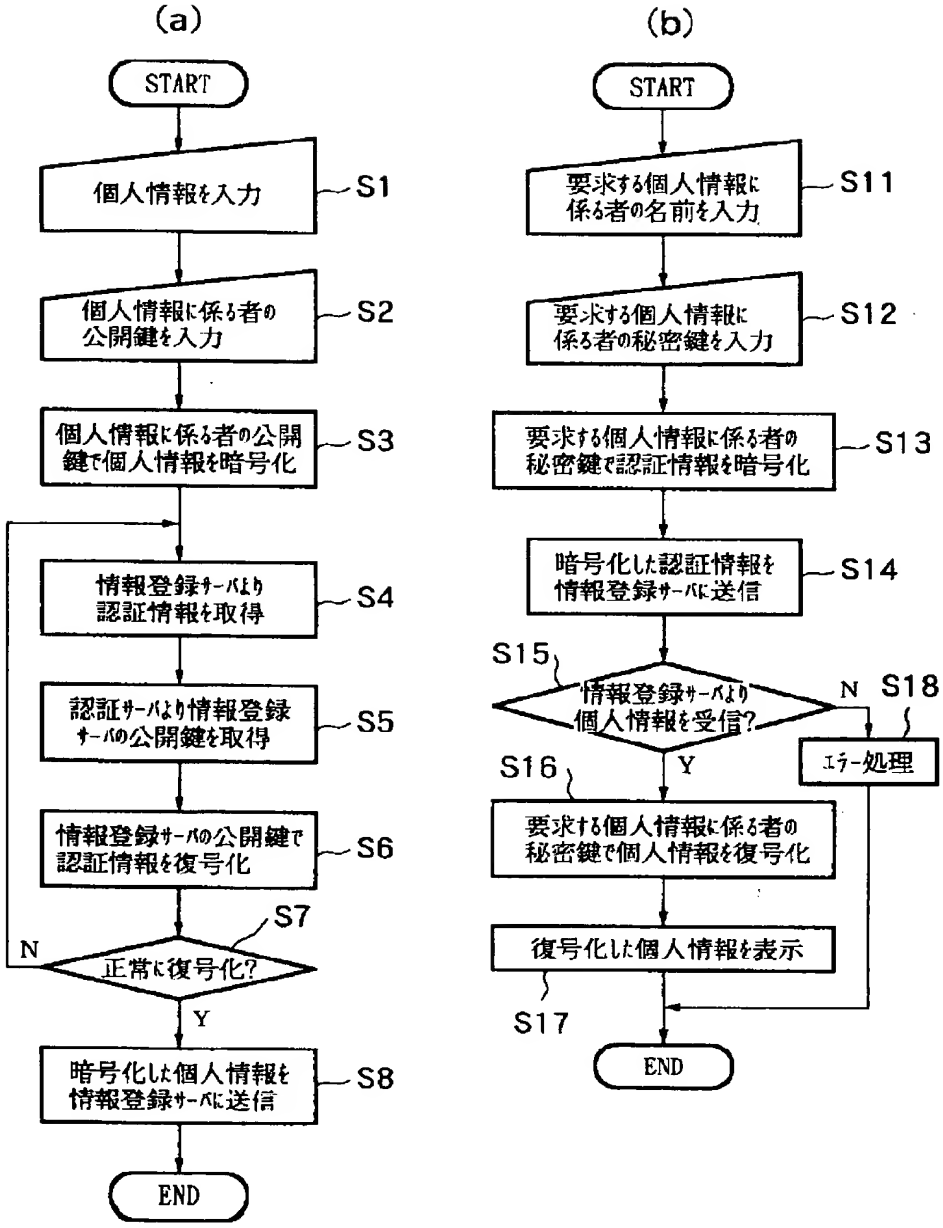
【図２】


演算処理装置
5
4
インターフェース部
9
主記憶装置
6
補助
記憶装置
7
キーボード
8
CRT制御装置
10
CRT
11

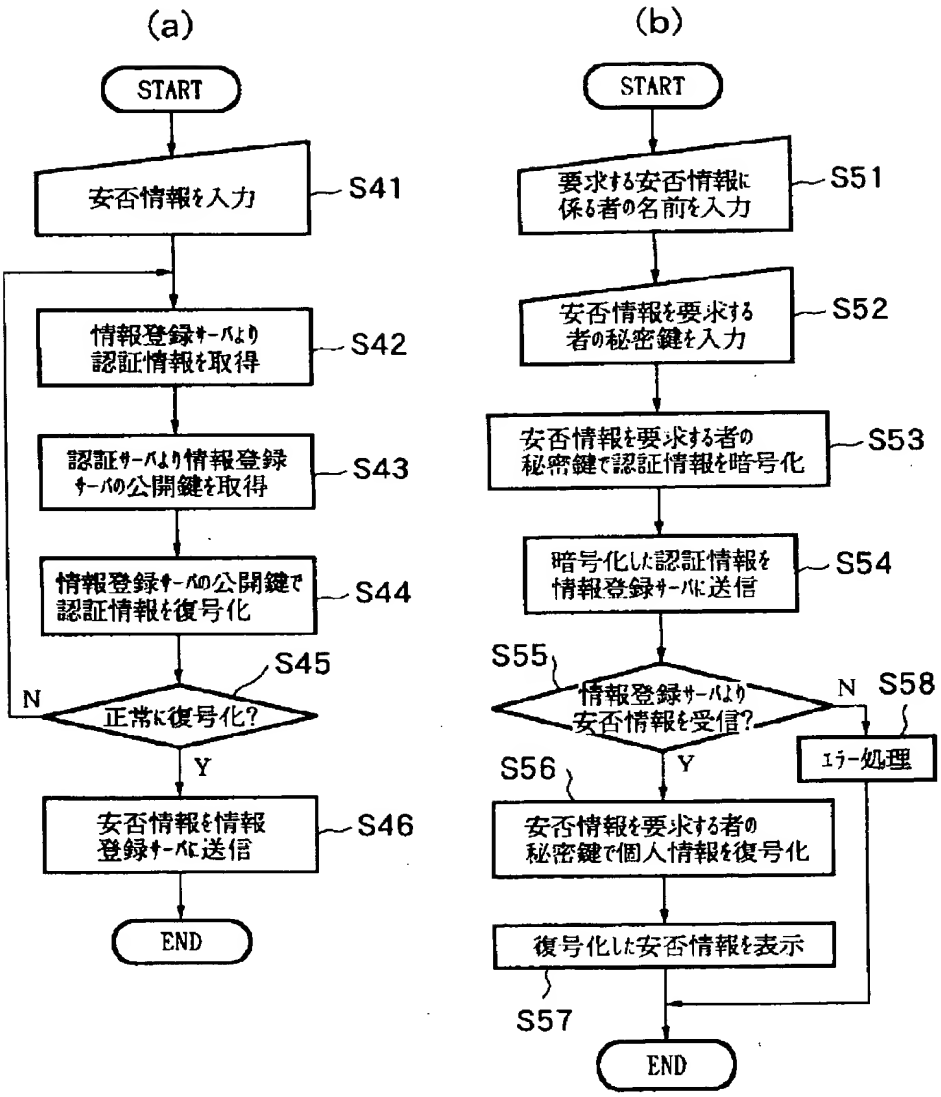
【図６】


(a)
START
情報登録サーバの秘密鍵で
認証情報を暗号化
S21
暗号化した認証情報を
入力端末に送信
S22
S23
入力端末より
個人情報を受信?
N
Y
S24
受信した個人情報を登録
S25
エラー処理
END
(b)
START
入力端末より認証情報を受信
S31
要求のあった個人情報に係る者の
公開鍵を認証サーバより取得
S32
要求のあった個人情報に係る者の
公開鍵で認証情報を復号化
S33
S34
正常に復号化?
N
Y
S35
該当する個人情報を
入力端末に送信
S36
エラー処理
END

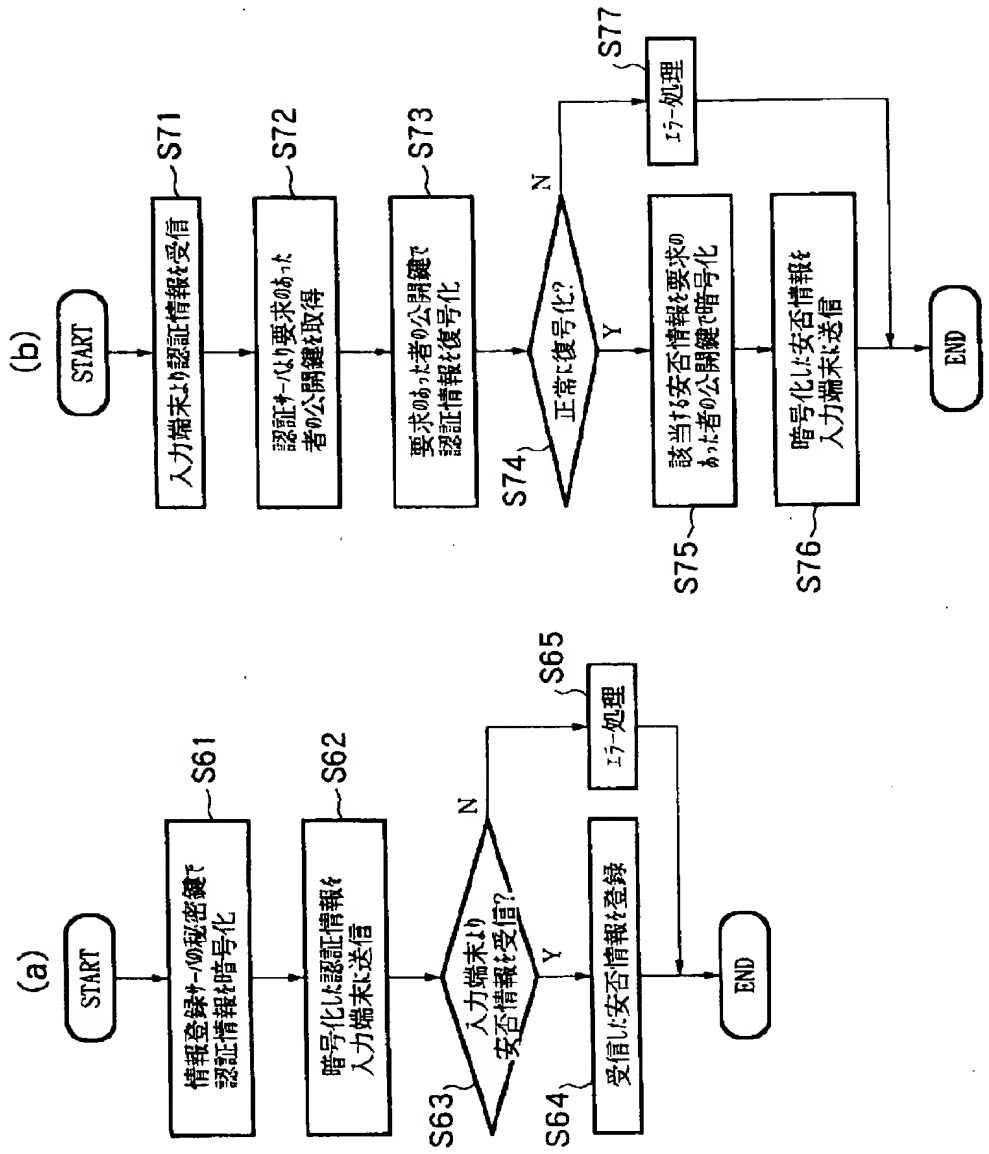
【図５】


(a)
START
個人情報を入力
S1
個人情報に係る者の公開鍵を入力
S2
個人情報に係る者の公開鍵で個人情報を暗号化
S3
情報登録サーバより認証情報を取得
S4
認証サーバより情報登録サーバの公開鍵を取得
S5
情報登録サーバの公開鍵で認証情報を復号化
S6
正常に復号化?
S7
N
Y
暗号化した個人情報を情報登録サーバに送信
S8
END
(b)
START
要求する個人情報に係る者の名前を入力
S11
要求する個人情報に係る者の秘密鍵を入力
S12
要求する個人情報に係る者の秘密鍵で認証情報を暗号化
S13
暗号化した認証情報を情報登録サーバに送信
S14
S15
情報登録サーバより個人情報を受信?
N
S18
エラー処理
Y
S16
要求する個人情報に係る者の秘密鍵で個人情報を復号化
復号化した個人情報を表示
S17
END

【図７】


(a)
START
安否情報を入力
S41
情報登録サーバより
認証情報を取得
S42
認証サーバより情報登録
サーバの公開鍵を取得
S43
情報登録サーバの公開鍵で
認証情報を復号化
S44
S45
N
正常に復号化?
Y
安否情報を情報
登録サーバに送信
S46
END
(b)
START
要求する安否情報に
係る者の名前を入力
S51
安否情報を要求する
者の秘密鍵を入力
S52
安否情報を要求する者の
秘密鍵で認証情報を暗号化
S53
暗号化した認証情報を
情報登録サーバに送信
S54
S55
情報登録サーバより
安否情報を受信?
N
S58
エラー処理
Y
S56
安否情報を要求する者の
秘密鍵で個人情報を復号化
復号化した安否情報を表示
S57
END

【図８】



フロントページの続き

(51)Int.Cl.[6]	識別記号	FI	
H04M 11/04		H04L 11/02	Z